УДК 681.3.06:519.248.681

Мельник С. В., канд. техн. наук. Тел. +380 (44) 241 11 21. E-mail: msvcontakt@gmail.com
(Навчально-науковий інститут інформаційної безпеки Національної академії Служби безпеки України)

МЕТОД ПОБУДОВИ ОДНОГО КЛАСУ БУЛЬОВИХ ФУНКЦІЙ ДЛЯ КРИПТОГРАФІЧНИХ ЗАСТОСУВАНЬ

Mel'nyk S. V. Method of constructing a class Boolean functions for cryptographic applications. The paper presents the method of constructing Boolean functions without prohibitions which reach the upper boundary nonlinearity algebraic normal form.We know, that the simultaneous achievement of limit values of known cryptographic properties of Boolean functions is not possible, so the methods which show interest, are methods of constructing Boolean functions with preset values for specific cryptographic scheme of block and streaming encryption algorithm.This method shows the interest in the tasks of building nonlinear knots complication of filter generators symmetric algorithms of stream encryption. Because the terms of use statistics and analytical methods of cryptanalysis cryptographic schemes of filter generators are relevant listed above properties. The justification of the proposed method based on estimates nonlinearity of Boolean functions with an odd number of arguments which have linear structures with 1 Heming's weight and known from cryptography and coding theory result of cryptographic properties of bent functions. The essence of method is to select the bent function with specified number of arguments , degree of nonlinearity algebraic normal form and input linear structure with 1 Heming's weight by such way ,that received function with an odd number of arguments is linear in one of the extreme arguments.

Keywords: Boolean function, prohibition of boolean function, De Bruijn graph, nonlinearity criteria for cryptographic functions, bent functions

Мельник С. В. Метод побудови одного класу бульових функцій для криптографічних застосувань. В роботі запропоновано метод побудови сильно рівноімовірних (без заборон) бульових функцій, які досягають верхньої границі нелінійності (відстані до класу афінних функцій) та забезпечують достатньо високий ступінь нелінійності алгебраїчної нормальної форми. Зазначений метод представляє інтерес в завданнях побудови нелінійних вузлів ускладнення фільтруючих генераторів симетричних алгоритмів потокового шифрування. Обґрунтування запропонованого методу базується на оцінках нелінійності бульових функцій з непарною кількістю аргументів, що мають лінійну структуру вагою 1, а також відомих із криптографії та теорії кодування результатів щодо криптографічних властивостей бент-функцій.

***Ключові слова*:** бульова функція, заборона бульової функції, граф Де-Брейна, нелінійність криптографічних функцій, бент-функції

Мельник С. В. Метод построения одного класса булевых функций для криптографических применений. В работе предложен метод построения сильно равновероятных (без запретов) булевых функций с верхней границей нелинейности (расстоянием к классу аффинных функций), обеспечивающих при этом достаточно высокую степень нелинейности полинома Жегалкина. Предложенный метод представляет интерес в задачах построения нелинейных узлов усложнения фильтрующих генераторов симметричных алгоритмов поточного шифрования. Обоснование предложенного метода базируется на оценках нелинейности булевых функций с нечетным количеством аргументов, имеющих линейную структуру веса 1, а также известных из криптографии и теории кодирования результатов относительно криптографических свойств бент-функций.

Ключевые слова: булева функция, запрет булевой функции, граф Де-Брейна, нелинейность криптографических функций, бент-функции

1. Вступ та постановка задачі

Методи сучасної криптографії та симетричної криптографії зокрема, є невід'ємною частиною сучасних телекомунікаційних та інформаційних технологій, що використовуються для забезпечення конфіденційності та цілісності інформаційних ресурсів, програмних засобів обробки і захисту інформації тощо. На сьогодні, в умовах розвитку відкритої (або громадської) криптографії та стандартизації у галузі криптографічного захисту інформації, достатньо багато уваги приділяється питанням розроблення, моделювання та оцінювання симетричних шифрів із практичним рівнем криптографічної стійкості. Одним із таких питань є тематика бульових функцій, які використовуються в якості нелінійних вузлів ускладнення

потокових та блокових алгоритмів шифрування. Оскільки роботу алгоритму шифрування, як правило, можна описати у вигляді системи бульових рівнянь, де невідомими є елементи ключових даних, а також систем бульових лінійних і нелінійних рівнянь. Показники ефективності рішення цих рівнянь (методів криптоаналізу) безпосередньо визначають рівень практичної криптографічної стійкості.

Звісно рівень практичної криптографічної стійкості є основною характеристикою алгоритмів шифрування, що визначається параметрами ефективності методів криптоаналізу, насамперед, такими як складність (кількість елементарних операцій) та надійність (імовірність успішного застосування). Методи криптоаналізу алгоритмів шифрування можна класифікувати згідно різних ознак. Однак в контексті статті представляють інтерес саме ті, що використовують імовірнісні способи лінеаризації бульових нелінійних рівнянь за рахунок аналітичних і статистичних підходів, а також мають за мету подальше застосування методів рішення систем бульових лінійних рівнянь чи методів направленого перебору ключових параметрів алгоритмів шифрування.

Тобто, криптографічні характеристики бульових функцій визначають показники складності та надійності методів криптоаналізу (рівень практичної криптографічної стійкості), відповідно, є актуальною потреба у розробці методів побудови бульових функцій із заданими криптографічними параметрами.

В статті запропоновано метод побудови сильно рівноімовірних бульових функцій з високими показниками нелінійності.

2. Аналіз літературних даних

Тематика криптографічних характеристик бульових функцій розглянута багатьма іноземними та вітчизняними фахівцями [1-16] та стосується, насамперед, методів побудови і оцінювання бульових функцій, що формують бієкції *S*-блоків алгоритмів блокового шифрування, які характеризують ефективність методів лінійного та дифереренційного криптоаналізу. Окремі положення наукових результатів зазначених авторів розкриті в основній частині роботи.

На основі аналізу літературних джерел, доцільно зазначити, що результати аналізу криптографічних характеристик бульових функцій свідчать про факт неможливості одночасного досягнення максимуму їх значень. Відповідно, представляють науковий та практичний інтерес методи побудови бульових функцій із криптографічними характеристиками, які є адаптованими до відповідних криптографічних схем алгоритмів потокового і блокового шифрування.

3. Мета і задачі дослідження

Мета роботи полягає в обґрунтуванні методу побудови бульових функцій для криптографічних схем фільтруючих генераторів алгоритмів потокового шифрування, що забезпечують сильну рівноімовірність та високі показники нелінійності. Для досягнення поставленої мети вирішувалися наступні завдання:

– аналіз відомих криптографічних характеристик бульових функцій та їх максимальних показників;

– визначення ефективного способу досягнення високих значень криптографічних характеристик для сильно рівноімовірних бульових функцій.

4. Статистичні та аналітичні характеристики бульових функцій

Звісно у якості вузлів ускладення потокових алгоритмів шифрування використовуються збалансовані (або рівно імовірні) бульові функції, оскільки в іншому випадку псевдовипадкова послідовність (гама) алгоритму шифрування та послідовність шифротексту не буде рівноімовірною. Відповідно, до таких алгоритмів можуть бути успішно застосовані методи безключового читання шифротексту.

Розглянемо ще одну статистичну характеристику, яка отримала назву заборон бульових функцій ([1-3]). Заборони бульових функцій потенційно можуть бути використані при застосуванні статистичних методів криптоаналізу потокових алгоритмів шифрування.

Припустимо є пристрій з фільтруючою функцією $f(\bar{x})$, $\bar{x} \in V_n(2)$, де $V_n(2)$ – визначає векторний простір розміром *n* над полем GF(2) наступного виду.

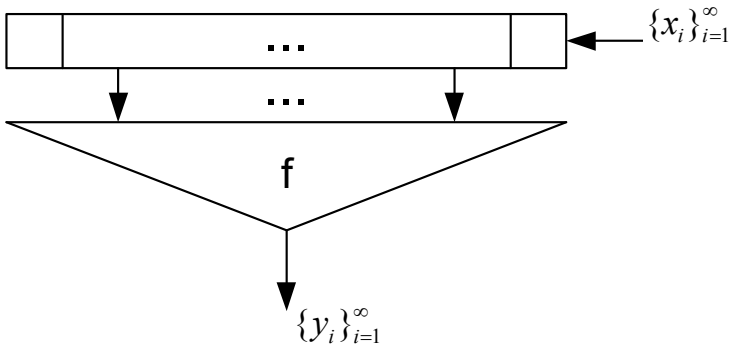

Рис. 1. Схема фільтруючого генератора

Вихідна послідовність цього пристрою описується системою бульових рівнянь: $y_i = f(x_i,...,x_{n+i+1})$, (*i*=1,2,…). Запишемо перші *m* рівнянь із цієї системи.

$$\begin{cases} y_1 = f(x_1,...,x_n) \\ y_2 = f(x_2,...,x_{n+1}) \\ \quad\quad ... \\ y_m = f(x_m,...,x_{n+m-1}) \end{cases}. \qquad (1)$$

У випадку, якщо існує таке натуральне *m* і вектор $(y_1,...,y_m) \in V_m(2)$, що представлена система несумісна, то функція *f* має заборону $y_1...y_m$ довжини *m*.

Бульова функція $f(\bar{x})$, $\bar{x} \in V_n(2)$ називається сильно рівноімовірною, якщо для будь-якого натурального *m* і будь-яких векторів $(y_1,...,y_m) \in V_m(2)$ система (1) має рівно 2^{n-1} рішень.

Доведено [1], що функція сильно рівноімовірна тоді і лише тоді, коли вона не має заборон.

Зрозуміло, що будь-яка сильно равноімовірна функція буде рівноімовірною, зворотня теза не завжди вірна.

Заборони бульових функцій були розглянуті на прикладі графів де-Брейна. Достатня (але не необхідна) умова відсутності заборон у бульовій функції полягає в тому, що граф де-Брейна цієї функції дихотомічний в пряму або зворотну сторону, що рівносильне лінійності функції хоча б за одним із крайніх аргументів.

Далі розглянемо ще одну криптографічну характеристику бульових функцій, що отримала назву нелінійності [4, 5].

В класичній математичній логіці найбільш вивченими є способи "точного" представлення бульових функцій. Однак в криптографічній практиці значний інтерес представляють також і нетрадиційні способи "наближеного" представлення бульових функцій.

Так, дистанцією між двома бульовими функціями [4] називається відстань Хеммінга між вектор-стовпчиками їх таблиць істинності, які визначаються наступним чином:

$$d(f_1, f_2) = |\{\bar{x} \in V_n(2) : f_1(\bar{x}) \neq f_2(\bar{x})\}|,$$

або

$$d(f_1, f_2) = \sum_{\bar{x} \in V_n(2)} f_1(\bar{x}) \oplus f_2(\bar{x}).$$

Дистанція функції $f(\bar{x})$, $\bar{x} \in V_n(2)$ до деякої лінійної функції $L_{\bar{w}}$ (де $\bar{w} \in V_n(2)$ і $L_{\bar{w}} = (\bar{w}, \bar{x})$) тісно пов'язана з *кореляційним коефіцієнтом* $C(f(\bar{x}), L_{\bar{w}})$ [4]:

$$d(f(\bar{x}), L_{\bar{w}}) = 2^{n-1}(1 - C(f(\bar{x}), L_{\bar{w}})),$$

де $$C(f(\bar{x}), L_{\bar{w}}) = 2^{-n} \sum_{\bar{x} \in V_n(2)} (-1)^{f(\bar{x}) \oplus \bar{w}\bar{x}} = 2^{-n} \hat{F}(\bar{w}),$$

$\bar{w}\bar{x}$ – скалярний добуток векторів $\bar{w}, \bar{x} \in V_n(2)$.

Тобто, дистанція бульової функції f до функції $L_{\bar{w}}$ може бути аналогічно виражена через перетворення Уолша-Адамара $\hat{F}(\bar{w})$:

$$d(f(\bar{x}), L_{\bar{w}}) = 2^{n-1} - \frac{1}{2}\hat{F}(\bar{w}).$$

Очевидно, що величина дистанції бульової функції f до функцій $L_{\bar{w}}$ та $L_{\bar{w}} \oplus 1$ співпадає.

Нелінійність бульової функції f характеризує її дистанцію до найкращого афінного наближення

$$N_f = \min d(f, l_i),$$
$$i = 0, 1, ..., 2^{n+1}$$

де l_i – функція, що послідовно обирається із всієї множини афінних функцій (множини лінійних функцій з одиницею).

Нелінійність бульової функції може бути також виражена через перетворення Уолша-Адамара:

$$N_f = d(f(\bar{x}), A) = 2^{n-1} - \frac{1}{2}\max_w \{|\hat{F}(\bar{w})|\}, \quad (2)$$

де A – множина афінних функцій від n змінних.

Тому дистанція $d(f(\bar{x}), A)$ досягає верхньої межі, якщо максимальне значення перетворення Уолша-Адамара $\max_w \{|\hat{F}(\bar{w})|\}$ приймає мінімально можливу на множені A величину.

Відповідно до теореми Парсеваля [4]:

$$\sum_{\bar{w} \in V_n(2)} \hat{F}(\bar{w}) = 2^{2n}. \quad (3)$$

Тому максимально можливе значення коефіцієнта $\hat{F}^2(\bar{w})$ дорівнює 2^{2n} і досягається лише на афінних функціях. Для будь-якої функції із множини бульових функцій від n

аргументів максимальне значення коефіцієнту $\hat{F}^2(\bar{w})$ не може бути менше за $2^{2n}/2^n = 2^n$. Нижнє значення досягається у випадку рівності значень $\hat{F}^2(\bar{w})$ для всіх векторів $\bar{w} \in V_n(2)$, відповідно, мінімальна величина $\max\limits_{w}\{|\hat{F}(\bar{w})|\} \geq \pm 2^{\frac{n}{2}}$.

Виходячи з того, що коефіцієнти перетворення Уолша-Адамара приймають значення лише із множини цілих чисел, то із (2) виходить, що нелінійність бульової функції з парною кількістю аргументів не перевищує величини [4, 5]

$$N_f \leq 2^{n-1} - 2^{\frac{n}{2}-1}. \tag{4}$$

Граничне значення досягається на функціях, які отримали назву *бент-функцій* [6], які активно вивчались в теорії кодування на протязі тривалого часу [7].

Так бульову функцію $f(x_1,\ldots,x_n)$ називають бент-функцією, якщо її перетворення Уолша-Адамара дорівнює $\hat{F}(\bar{w}) = \pm 2^{\frac{n}{2}}$ для всіх векторів $\bar{w} \in V_n(2)$.

В роботі [7] доведено, що бент-функції мають обмеження на аналітичну характеристику бульових функцій – ступінь нелінійності алгебраїчної нормальної форми бульової функції *deg* (*f*) (ступінь нелінійності поліному Жегалкіна функції $f(x_1,\ldots,x_n)$), яка визначає складність аналітичних методів криптоаналізу алгоритмів шифрування. Так було доведено, що ступінь нелінійності бент-функцій від *n* аргументів ($n>2$), не превищує $\frac{n}{2}$, відповідно, відносно цієї характеристики бент-функції не є максимально нелінійними.

В контексті сказаного звернемо увагу на ще одну статистичну характеристику – клас бульових функцій з лінійними структурами. Функція $f(\bar{x})$, $\bar{x} \in V_n(2)$ має лінійну структуру [8], якщо для всіх $\bar{x} \in V_n(2)$ виконується умова:

$$f(\bar{x}) = f(\bar{x} \oplus \bar{\alpha}) \text{ або } f(\bar{x}) \neq f(\bar{x} \oplus \bar{\alpha}),$$

для деякої константи $\bar{\alpha} \in V_n(2)$.

Крім того, має місце визначення абсолютної нелінійності бульових функцій (по відношенню до лінійних структур). Бульова функція $f(x_1,\ldots,x_n)$ є абсолютно нелінійною, якщо для будь-якого вектору $\bar{\alpha} \neq 0$ справедливий вираз: $\sum\limits_{\bar{x} \in V_n(2)} f(\bar{x}) \oplus f(\bar{x} \oplus \bar{\alpha}) = 2^{n-1}$.

В роботі [8] було доведено, що клас абсолютно нелінійних функцій співпадає з класом бент-функцій. Тобто бент-функції мають максимальну відстань як до класу афінних функцій, так і до класу функцій з лінійними структурами.

Альтернативне визначення бульових бент-функцій [9] було надано в термінах комбінаторних структур, що отримали назву множин різниці. Функція f: $V_n(2) \to V(2)$ є бент-функцією, якщо множина $S=\{\bar{x} : f(\bar{x}) = 1\}$ представляє собою множину обчислених різниць в $V_n(2)$ з параметрами (2^n, $2^{n-1} \pm 2^{\frac{n}{2}-1}$, $2^{n-2} \pm 2^{\frac{n}{2}-1}$). Таким чином, бент-функції не можуть бути рівноімовірними та не можуть бути застосовані як нелінійні вузли ускладнення алгоритмів шифрування.

У зв'язку з цим постає питання про граничну оцінку нелінійності для бульових функцій з непарною кількістю аргументів та питання рівноімовірності зазначених функцій.

Зазначимо, що для бульової функції $f(x_1, x_2, ..., x_n)$ з непарною кількістю аргументів *n*, кількість однакових коефіцієнтів перетворення Уолша-Адамара $\hat{F}^2(\bar{w})$ буде однозначно

менше 2^n. Таким чином, справедливий вираз $\max\limits_{w}\{|\widehat{F}^2(\overline{w})|\} > 2^n$, і для визначення величини нелінійності функції необхідно визначити найменше значення $\widehat{F}^2(\overline{w})$, яке перевищує 2^n.

Із виразу (3) виходить, що значення $\max\limits_{w}\{|\widehat{F}^2(\overline{w})|\}$ дорівнює 2^{n+1} для всіх $2^{2n}/2^{n+1} = 2^{n-1}$ векторів $\overline{w} \in V_n(2)$. Звідси зрозуміло, що для функцій з мінімальною величиною $\max\limits_{w}\{|\widehat{F}(\overline{w})|\}$, вірний вираз:

$$\widehat{F}(\overline{w}) = \pm 2^{\frac{n+1}{2}}, \tag{5}$$

для довільних 2^{n-1} векторів $\overline{w}$ из $V_n(2)$.

Враховуючи (2, 5), зрозуміло, що для величини нелінійності бульової функції від непарної кількості аргументів справедливий наступний вираз

$$N_f \le 2^{n-1} - 2^{\frac{n+1}{2}-1}. \tag{6}$$

Достатньо часто при оцінці нелінійності бульових функцій зручно оперувати відносною величиною нелінійності $\Delta_f = \dfrac{N_f}{2^n}$. Звісно з точки зору криптографічних застосувань найбільш цікавими будуть функції з максимальною величиною Δ_f.

Розглянута верхня оцінка нелінійності бульової функції від непарної кількості аргументів дозволяє сформулювати наступне твердження.

Твердження 1. Максимально можливе значення величини відносної нелінійності Δ_{f_2} функції $f_2(x_1, x_2, ..., x_{n+1})$ з непарною кількістю аргументів співпадає з максимально можливим значенням величини Δ_{f_1} функції $f_1(x_1, x_2, ..., x_n)$.

Доведення.

Враховуючи (4), величина Δ_{f_1} для функції $f_1(x_1, x_2, ..., x_n)$ приймає максимальне значення

$$\Delta_{f_1} = \frac{2^{n-1} - 2^{\frac{n}{2}-1}}{2^n} = \frac{2^n - 2^{\frac{n}{2}}}{2^{n+1}}.$$

Відповідно, з урахуванням (6), приходимо до висновку, що відносна величина нелінійності функції $f_2(x_1, x_2, ..., x_n)$ дорівнює

$$\Delta_{f_2} = \frac{2^n - 2^{\frac{n+2}{2}-1}}{2^{n+1}} = \frac{2^n - 2^{\frac{n}{2}}}{2^{n+1}},$$

тобто $\Delta_{f_1} = \Delta_{f_2}$.

Твердження доведено.

Далі знову звернемо увагу на клас бульових функцій з лінійними структурами. І для нас представляє інтерес випадок, коли $\|\overline{\alpha}\|$=1.

Як відомо під фіктивним аргументом бульової функції $f(\bar{x})$, $\bar{x} \in V_n(2)$ розуміється аргумент x_i ($i=1,\ldots,n$), для якого виконується умова

$$f(x_1,...,x_{i-1},0,x_{i+1},...,x_n) = f(x_1,...,x_{i-1},1,x_{i+1},...,x_n),$$

для всіх наборів нефіксованих аргументів.

Зауважимо, що, якщо функція $f(x_1, x_2,..., x_n)$ має k фіктивних аргументів, то видаляючи всі фіктивні аргументи, ми отримуємо функцію від n-k змінних. Очевидно, що величина Δ_f функції $f(x_1, x_2,..., x_n)$ визначена величиною $\Delta_{f'}$ підфункції $f'(x_1, x_2,..., x_{n-k})$, що отримується після видалення всіх k фіктивних змінних.

Функція $f(\bar{x})$, $\bar{x} \in V_n(2)$ лінійна по аргументу x_i (i={1,…,n}), якщо

$$f(x_1,...,x_{i-1},0,x_{i+1},...,x_n) \neq f(x_1,...,x_{i-1},1,x_{i+1},...,x_n)$$

для всіх наборів нефіксованих аргументів.

Твердження 2. Припустимо $\hat{F}_1(\bar{w})$ і $\hat{F}_2(\bar{w})$, $\bar{w} \in V_n(2)$ перетворення Уолша-Адамара бульових функцій $f_1(\bar{x})$ і $f_2(\bar{x})$, $\bar{x} \in V_n(2)$, виду: $f_1(x_1,...,x_n) = f_1(x_1,...,x_{i-1},x_{i+1},...,x_n)$, $f_2(x_1,...,x_n) = f_1(x_1,...,x_{i-1},x_{i+1},...,x_n) \oplus x_i$ ($i=\{1,\ldots,n\}$). Тоді має місце вираз:

$$\hat{F}_2(\bar{w}) = \hat{F}_1(\bar{w} \oplus \bar{c}_i), \tag{7}$$

де $\| \bar{c}_i \| = 1$, $\bar{c}_i \in V_n(2)$ – бульовий вектор з одиницею в і-й координаті.

Доведення.

Розглянемо вираз

$$\hat{F}_2(\bar{w}) = \sum_{\bar{x} \in V_n(2)} (-1)^{f_1(\bar{x}) \oplus x_l \oplus \bar{w}\bar{x}} .$$

$$\hat{F}_1(\bar{w} \oplus \bar{c}_i) = \sum_{\bar{x} \in V_n(2)} (-1)^{f_1(\bar{x}) \oplus (w \oplus c_i)} = \sum_{\bar{x} \in V_n(2)} (-1)^{f_1(\bar{x}) \oplus w_1 x_1 \oplus ... \oplus (w_i \oplus 1) x_i \oplus ... \oplus w_n x_n} =$$

$$= \sum_{\bar{x} \in V_n(2)} (-1)^{f_1(\bar{x}) \oplus x_l \oplus \bar{w}\bar{x}} = \hat{F}_2(\bar{w}) .$$

Твердження доведено.

Таким чином, враховуючи вираз (7), можна стверджувати, що відносно характеристики нелінійності перетворення Уолша-Адамара функцій $f_1(\bar{x})$ і $f_2(\bar{x})$ змінюється несуттєво.

Наслідок 1. Відносна нелінійність функцій $f_1(x_1,...,x_n) = f_1(x_1,...,x_{i-1},x_{i+1},...,x_n)$ та $f_2(x_1,...,x_n) = f_1(x_1,...,x_{i-1},x_{i+1},...,x_n) \oplus x_i$ ($i=\{1,\ldots,n\}$) співпадає за величиною, тобто $\Delta_{f_1} = \Delta_{f_2}$.

Наслідок 2. Величина відносної нелінійності функції $f(\bar{x})$, $\bar{x} \in V_n(2)$ з k лінійними складовими і підфункції $f'(x_1, x_2, ..., x_{n-k})$, отриманої в результаті фіксації k лінійних аргументів, співпадають.

5. Метод побудови сильно рівноімовірних бульових функцій, які досягають верхньої границі нелінійності

Твердження 3. Функція $f(\bar{x})$, $\bar{x} \in V_n(2)$ з фіктивним або лінійним аргументом x_i (i={1,…,n}) має граничний рівень нелінійності N_f тоді і лише тоді, коли n непарне і підфункція $f'(\bar{x})$, яка отримана в результаті фіксації аргументу x_i, має максимум $N_{f'}$, тобто є бент-функцією.

Твердження 4. Припустимо f будь-яка бент-функція ві n аргументів. Тоді функції виду

$$g(x_1, ..., x_{n+1}) = x_1 \oplus f(x_2, ..., x_{n+1})$$

та

$$g(x_1, ..., x_{n+1}) = f(x_1, ..., x_n) \oplus x_{n+1}$$

є бульовими сильно рівноімовірними функціями (без заборон), які мають максимальну величину нелінійності N_g для функцій від $n+1$ аргументів.

Твердження 4 лежить в основі методу побудови сильно рівноімовірних бульових функцій з максимально можливим значенням не лінійності. Ступінь нелінійності алгебраїчної нормальної форми таких функцій (включаючи ступінь нелінійності можливих підфункцій) визначається обраною структурою бент-функцій.

Необхідно зазначити, що ні повного опису бент-функцій, ні асимптотики їх числа на сьогодні не отримано. Однак, в багатьох публікаціях запропоновані описи різних класів бент-функцій із фіксованою структурою, деякі з них є прийнятними для використання у запропонованому в роботі методі. Мова йде про класи еквівалентних бент-функцій відносно групи G (взаємно однозначних перетворень множини $V_n(2)$ $f_2(x_1, ..., x_n) = f_1(g(x_1, ..., x_n))$, де $g \in G$). Однотипні функції представляють собою одну логічну форму, записану в різних системах координат, тому значна частина властивостей бульових функцій залишається незмінною в середині типу, або змінюється несуттєво.

6. Висновки

Опираючись на відомі результати криптоаналізу потокових алгоритмів шифрування, які побудовані на нелінійних вузлах ускладнення фільтруючих генераторів, можна дійти висновку, що у цьому випадку найбільш вагомими криптографічними характеристиками бульових функцій є відсутність заборон, максимальна нелінійність та ступінь нелінійності ($\frac{n}{2}$), який буде достатнім при відповідному значені n. Тому запропонований метод побудови одного класу бульових функцій для криптографічних застосувань є у достатній мірі прийнятним з точки зору сучасної криптографічної практики.

Література

1. Сумароков С. Н. Запреты двоичных функций и обратимость одного класса кодирующих устройств / С. Н. Сумароков // Обозрение прикл. и промышл. матем. Сер. дискретн. матем. – 1994. – Т.1, вып. 1. – С. 33-55.

2. Колесников О. В. Использование запретов двоичных функций при решении систем уравнений / О. В. Колесников // Обозрение прикл. и промышл. матем. Сер. дискретн. матем. – 1995. – Т.2, вып.3. – С. 483-493.

3. Рябоконь Д. В. Алгоритм поиска запретов булевы функций / Д. В. Рябоконь // Прикладная дискретная математика. Приложение. – 2013. – №6. – С. 123-125.

4. Meier W. and Staffelbach O. Nonlinearity criteria for cryptographic functions. LNCS 434; Proc. Eurocrypt'89.

5. Seberry J. Zhang X. M. and Zheng Y. Relationships among nonlinearity criteria. Presented at Eurocrypt'94.

6. Rothaus O. On bent Functions. J. Combinatorial Theory, 1976.

7. Дж. Мак-Вильямс. Теория кодов, исправляющих ошибки / Дж. Мак-Вильямс, Н. Дж. А. Слоэн. – Москва : Связь, 1976.

8. Evertse J.H. Linear structures in block ciphers. LNCS 304 (1987).

9. R. McFarland, "A family of difference sets in noncyclic groups", J. Comb. Theory, Ser. A (1973).

10. Логачев О. А. Булевы функции в теории кодирования и криптологии / О. А. Логачев, А. А. Сальников, В. В. Ященко В.В. – Москва : МЦНМО, 2004. 470 с.

11. Кузнецов А. А. Анализ известных методов построения высоко нелинейных булевых функций / А. А. Кузнецов, Ю. А. Избенко, А. А. Юкальчук // Вісник НТУ «ХПІ» Збірник наукових праць. – Харків: НТУ «ХПІ». - 2004. - №18. – С. 91-96.

12. Горбенко И. Д. Исследование аналитических и статистических свойств булевых функций криптоалгоритма Rijndael (FIPS 197) / И. Д. Горбенко, А. В. Потий, Ю. А. Избенко //Радиотехника. Всеукраинский межведомственный научно-технический сборник. – 2004. – № 126. – С. 132-138.

13. Кузнецов А. А. Метод построения криптографически стойких булевых функций на основе градиентного спуска / А. А. Кузнецов, Ю. А. Избенко, И. В. Московченко // Збірник наукових праць ХУПС. – Х.: ХУПС, 2007. – Вип. 1 (13). – С. 63-66.

14. Кузнецов А. А. Методика исследования эффективности нелинейных узлов замен симметричных криптографических средств защиты информации / А. А. Кузнецов, Ю. А. Избенко, И. В. Московченко // Збірник наукових праць ДонІЗТ. – Донецьк: ДонІЗТ, 2008. – № 14. – С. 74-81.

15. Алексеев Е. К. О некоторых мерах нелинейности булевых функций / Е. К. Алексеев // Прикладная дискретная математика. – 2011. – № 2(12). – С. 5-16.

16. Алексейчук А. Н. Алгебраически вырожденные приближения булевых функций / А. Н. Алексейчук, С. Н. Конюшок // Кибернетика и системный анализ. – 2014. – Т. 50. – № 6. – С. 3-14.

Дата надходження в редакцію: 14.07.2015 р. Рецензент: д.т.н., проф. О. О. Скопа